

1/5/1 (Item 1 from file: 351)
 DIALOG(R) File 351: DERWENT WPI
 (c) 2000 Derwent Info Ltd. All rts. reserv.

010813429 **Image available**
 WPI Acc No: 96-310382/199632
 XRPX Acc No: N96-260818

Processor-controlled exchange of cryptographic keys, e.g. in mobile communications - exchanging keys between network computer and user computer using Diffie-Hellman key exchange principle, and testing responses at both computers

Patent Assignee: SIEMENS AG (SIEI)
 Inventor: HORN G; KESSLER V; MUELLER K
 Number of Countries: 024 Number of Patents: 005
 Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 19514084	C1	19960711	DE 1014084	A	19950413	H04L-009/00	199632 B
KR 98703838	A	19981205	WO 96DE591	A	19960403	H04L-009/08	200006
			KR 97707238	A	19971013		
WO 9632791	A1	19961017	WO 96DE591	A	19960403	H04L-009/08	199647
EP 820670	A1	19980128	EP 96908004	A	19960403	H04L-009/08	199809
			WO 96DE591	A	19960403		
JP 10510692	W	19981013	JP 96530635	A	19960403	H04L-009/08	199851
			WO 96DE591	A	19960403		

Priority Applications (No Type Date): DE 1014084 A 19950413

Cited Patents: Jnl.Ref; EP 393806

Patent Details:

Patent	Kind	Lan	Pg	Filing	Notes	Application	Patent
DE 19514084	C1		10				
KR 98703838	A			Based on		WO 9632791	
WO 9632791	A1	G	27				
Designated States (National): CN JP KR RU UA US							
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC							
NL PT SE							
EP 820670	A1	G		Based on		WO 9632791	
Designated States (Regional): AT CH DE ES FR GB IT LI							
JP 10510692	W		26	Based on		WO 9632791	

Abstract (Basic): DE 19514084 C

Cryptographic keys are exchanged by generating a first coincidence number on the network computer (N). A first message is transmitted from a network computer to a subscriber computer which generates a second coincidence number. The second coincidence number generates a value which enables an open network key. The subscriber computer calculates an encrypted term (VT1). The subscriber computer generates a second message which contains at least the value generated by the second coincidence number, the first encrypted term, and the first response (A).

The second message is transmitted from the subscriber computer to the network computer. The first response is tested in the network computer. The network computer then sends a third message which includes at least a second response (B) which is tested in the subscriber computer.

USE/ADVANTAGE - Confidential information system. Explicit authentication of code messages by network computer and subscriber computer.

Dwg.1a/2

Title Terms: PROCESSOR; CONTROL; EXCHANGE; CRYPTOGRAPHIC; KEY; MOBILE; COMMUNICATE; EXCHANGE; KEY; NETWORK; COMPUTER; USER; COMPUTER; KEY; EXCHANGE; PRINCIPLE; TEST; RESPOND; COMPUTER

Derwent Class: P85; T01; W01

International Patent Class (Main): H04L-009/00; H04L-009/08

International Patent Class (Additional): G06F-012/14; G09C-001/00; H04L-009/32

(51) Int.Cl. ⁶	識別記号	F I
H 0 4 L 9/08		H 0 4 L 9/00 6 0 1 D
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00 6 0 1 E 6 7 5 B

審査請求 有 予備審査請求 有 (全 26 頁)

(21) 出願番号 特願平8-530635
 (86) (22) 出願日 平成8年(1996)4月3日
 (85) 翻訳文提出日 平成9年(1997)10月13日
 (86) 国際出願番号 PCT/DE96/00591
 (87) 国際公開番号 WO96/32791
 (87) 国際公開日 平成8年(1996)10月17日
 (31) 優先権主張番号 195 14 084. 2
 (32) 優先日 1995年4月13日
 (33) 優先権主張国 ドイツ (DE)
 (81) 指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), CN, JP, KR, RU, UA, US

(71) 出願人 シーメンス アクチエンゲゼルシャフト
 ドイツ連邦共和国 D-80333 ミュンヘン
 ヴィッテルスバッハープラッツ 2
 (72) 発明者 ギュンター ホルン
 ドイツ連邦共和国 D-81541 ミュンヘン
 エードゥアルト-シュミット-シュトラッセ 16
 (72) 発明者 クラウス ミュラー
 ドイツ連邦共和国 D-81539 ミュンヘン
 ラインターラー シュトラッセ 15
 (74) 代理人 弁理士 矢野 敏雄 (外3名)

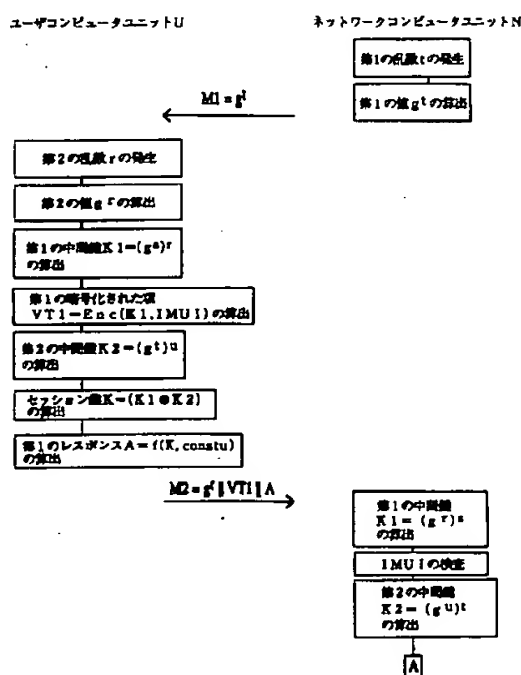
最終頁に続く

(54) 【発明の名称】 ユーザコンピュータユニットUとネットワークコンピュータユニットNの間における暗号鍵のコンピュータ支援交換方法

(57) 【要約】

本発明は暗号鍵の交換方法に関する。これによれば伝送されるメッセージの長さが低減され、この方法のセキュリティ特性は公知の方法よりも著しく拡大される。ネットワークコンピュータユニットとユーザコンピュータユニットにおいて、発せられた乱数に依存して第1の中間鍵と第2の中間鍵が生成される。これら第1の中間鍵と第2の中間鍵とをビットごとに排他OR結合することにより、セッション鍵が算出される。この鍵は絶対に平文では伝送されない。たとえば対称暗号化関数、ハッシュ関数または一方方向性関数とすることのできる所定の関数を利用することにより、ネットワークコンピュータユニットとユーザコンピュータユニットが互いに認証され合う。

FIG 1a



【特許請求の範囲】

1. ユーザコンピュータユニット (U) とネットワークコンピュータユニット (N) の間における暗号鍵のコンピュータ支援交換方法において、

ネットワークコンピュータユニット (N) 内で第1の乱数 (t) を生成し、

ネットワークコンピュータユニット (N) 内で該第1の乱数 (t) から、1つの有限群における生成要素 (g) を用いることにより第1の値 (g^t) を算出し、

ネットワークコンピュータユニット (N) において、少なくとも該第1の値 (g^t) を含む第1のメッセージ (M1) を生成し、

該第1のメッセージ (M1) をネットワークコンピュータユニット (N) からユーザコンピュータユニット (U) へ伝送し、

ユーザコンピュータユニット (U) において第2の乱数 (r) を生成し、

ユーザコンピュータユニット (U) において該第2の乱数 (r) から、1つの有限群における生成要素 (g) を用いることで第2の値 (g^r) を生成し、

ユーザコンピュータユニット (U) において、前記第2の乱数 (r) によりネットワーク公開鍵 (g

s) を累乗することで第1の中間鍵 (K_1) を算出し、

ユーザコンピュータユニット (U) において、ユーザ秘密鍵 (u) により前記第1の値 (g^t) を累乗することで第2の中間鍵 (K_1) を算出し、

ユーザコンピュータユニット (U) において、前記の第1の中間鍵 (K_1) と第2の中間鍵 (K_2) との結合によりセッション鍵 (K) を算出し、

ユーザコンピュータユニット (U) において、少なくとも前記第2の値 (g^r) を含む第2のメッセージ (M2) を生成し、

該第2のメッセージ (M2) をユーザコンピュータユニット (U) からネットワークコンピュータユニット (N) へ伝送し、

ネットワークコンピュータユニット (N) において、ネットワーク秘密鍵 (s) により前記第2の値 (g^r) を累乗することで第1の中間鍵 (K_1) を算出し、

ネットワークコンピュータユニット (N) において、前記第1の乱数 (t) によりユーザ公開鍵 (g^u) を累乗することで第2の中間鍵 (K2) を算出し、

ネットワークコンピュータユニット (N) において、前記第1の中間鍵 (K1) と第2の中間鍵 (K2) との結合によりセッション鍵 (K) を算出することを特徴とする、

ユーザコンピュータユニット (U) とネットワークコンピュータユニット (N) の間における暗号鍵のコンピュータ支援交換方法。

2. ユーザコンピュータユニット (U) において、該ユーザコンピュータユニット (U) の身元識別情報 (IMUI) を前記第1の中間鍵 (K1) を用い暗号化関数 (Enc) を利用して暗号化することで、第1の暗号化された項 (VT1) を算出し、

前記第2のメッセージ (M2) に付加的に少なくとも該第1の暗号化された項 (VT1) を含ませ、

ネットワークコンピュータユニット (N) において該第1の暗号化された項 (VT1) を解読し、

ネットワークコンピュータユニット (N) においてユーザコンピュータユニット (U) の身元識別情報 (IMUI) を検査する、

請求項1記載の方法。

3. ユーザコンピュータユニット (U) において、前記第1の中間鍵 (K1) と第2の中間鍵 (K2) とのビットごとの排他OR結合によりセッション鍵 (K) を算出し、

ネットワークコンピュータユニット (N) において、前記第1の中間鍵 (K1) と第2の中間鍵 (K2) とのビットごとの排他OR結合によりセッション鍵 (K) を算出する、

請求項1または2記載の方法。

4. ユーザコンピュータユニット (U) において、ユーザ定数 (constu) と前記セッション鍵 (K) に対し関数 (f) を適用することで第1のレスポンス

(A) を生成し、

前記第2のメッセージ(M2)に付加的に少なくとも該第1のレスポンス(A)を含ませ、

ネットワークコンピュータユニット(N)において該第1のレスポンス(A)を検査する、

請求項1～3のいずれか1項記載の方法。

5. ネットワークコンピュータユニット(N)において、ネットワーク定数(constn)とセッション鍵(K)に対し関数(f)を適用することで第2のレスポンス(B)を生成し、

少なくとも該第2のレスポンスを含む第3のメッセージ(M3)をネットワークコンピュータユニット(N)からユーザコンピュータユニット(U)へ伝送し、

ユーザコンピュータユニット(U)において該第2のレスポンス(B)を検査する、

請求項1～4のいずれか1項記載の方法。

6. 方法の開始にあたり認証メッセージをユーザコンピュータユニット(U)からネットワークコンピュータユニット(N)へ伝送し、該認証メッセージには認証コンピュータユニットにおける少なくとも1

つの識別情報が含まれ、該識別情報からユーザコンピュータユニット(U)により検証可能なネットワーク認証子(CertN)を送出させる、

請求項1～5のいずれか1項記載の方法。

7. 前記第1のメッセージ(M1)には、ネットワークコンピュータユニット(N)におけるネットワークコンピュータ鍵(g_s)のネットワーク認証子(CertN)が付加的に含まれ、

ユーザコンピュータユニット(U)において該ネットワーク認証子(CertN)を検証し、

ユーザコンピュータユニット(U)において、該ユーザコンピュータユニット(U)におけるユーザ公開鍵(g_u)のユーザ認証子(CertU)を前記第

2 の中間鍵 (K1) を用い暗号化関数 (Enc) を利用して暗号化することで第1の暗号化された項 (VT1) を生成し、

ネットワークコンピュータユニット (N) において該ユーザ認証子 (Cert) を検証する、

請求項1～6のいずれか1項記載の方法。

8. 前記関数 (f) は対称暗号化アルゴリズム、ハッシュアルゴリズムまたは一方向性関数であり、

ネットワークコンピュータユニット (N) における前記第1のレスポンス (A) の検査にあたり、前記関数 (f) をユーザ定数 (constu) とネットワークコンピュータユニット (N) 内で算出され

たセッション鍵 (K) とに対し適用し、その結果を前記第1のレスポンス (A) との整合性について検査し、

ユーザコンピュータユニット (U) における前記第2のレスポンス (B) の検査にあたり、前記関数 (f) をネットワーク定数 (constn) とユーザコンピュータユニット (U) 内で算出されたセッション鍵 (K) とに対し適用し、その結果を前記第2のレスポンス (B) との整合性について検査する、

請求項1～7のいずれか1項記載の方法。

9. 前記関数 (f) は対称暗号化アルゴリズムであり、

ネットワークコンピュータユニット (N) における前記第1のレスポンス (A) の検査にあたり、該第1のレスポンス (A) をネットワークコンピュータユニット (N) において該ネットワークコンピュータユニット (N) 内で算出されたセッション鍵 (K) を用いて解読し、解読されたユーザ定数 (constu') を前記ユーザ定数 (constu) と比較し、

ユーザコンピュータユニット (U) における前記第2のレスポンス (B) の検査にあたり、該第2のレスポンス (B) をユーザコンピュータユニット (U) において該ユーザコンピュータユニット (U

) 内で算出されたセッション鍵 (K) を用いて解読し、解読されたネットワーク

定数 (const n') を前記ネットワーク定数 (const n) と比較する、
請求項1～8のいずれか1項記載の方法。

【発明の詳細な説明】

ユーザコンピュータユニットJとネットワークコンピュータユニットNの間における暗号鍵のコンピュータ支援交換方法

情報技術システムは様々な脅威に晒されている。たとえば伝送された情報が、権限のない第三者により盗み出されて変えられてしまうおそれがある。また、2つの通信パートナー間における別の脅威として挙げられるのが、一方の通信パートナーの偽の識別子を偽造することである。

これらの脅威やさらに別の脅威は種々のセキュリティメカニズムにより対処され、それによって情報技術システムがそれらの脅威から保護されるようにしている。安全性のために利用される1つのセキュリティメカニズムは伝送データの暗号化である。この場合、2つの通信パートナー間の通信交渉におけるデータを暗号化できるようにする目的で、オリジナルのデータを伝送する前に、暗号化を準備処理する第1のステップを実行する必要がある。このステップはたとえば次のようなものとすることができる。すなわち、両方の通信パートナーを1つの暗号化アルゴリズムに向けて合意させ、必要に応じて共通の秘密鍵の取り決めを行わせる。

暗号化によるセキュリティメカニズムが重要な意味をもつのは移動無線システムにおいてである。それというのも、このようなシステムにおいて伝送されるデータというのは、付加的に特別な手間をかけずとも第三者により盗み出せるからである。

したがって、情報技術システムのセキュリティが保証されるよう、公知のセキュリティメカニズムの選択を行って、それらのセキュリティメカニズムを適切に組み合わせ、さらに通信プロトコルを指定しなければならない。

暗号鍵のコンピュータ支援交換を行うための種々の非対称方式が公知である。移動無線システムに適した非対称方式は、A. Aziz, W. Diffie 著の "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, p. 25-31, および M. Beller 著の "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and

Authentication for Personal Communications, P&A JEM 1993, p. 1-11 である。

A. Aziz, W. Diffie 著の "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, p. 25-31 に記載されている方法は、明らかにローカルネットワークに係わるものであり、暗号鍵交換にあたり各通信パートナーのコンピュータユニットに対し、著しく高い所要計算能力を課すものである。

しかもこの方法の場合、本発明による方法よりも大きな伝送キャパシティが必要とされる。それというのも、メッセージの長さが本発明による方法の場合よりも長いからである。

また、M. Beller 著の "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, p. 1-11 は、いくつかの基本的なセキュリティメカニズムを統合していない。この場合、ユーザによる明示的なネットワークの認証が実現されない。しかもこの場合、ユーザからネットワークへ伝送される鍵は、ネットワークによりユーザに対し受領確認されない。さらに、ネットワークのための鍵の更新（アップデート）も行われない。この方法のさらに別の欠点は、ユーザによる鍵の暗黙的な認証がラビン方式に限られていることである。これにより、この方法はフレキシブルな適用の点で制限されてしまう。しかも、伝送データが疑う余地のないものであることを保証するセキュリティメカニズムも設けられていない。このことは殊に、移動無線システムに関する疑う余地のない料金決済を作成する場合にも重大な欠点となる。また、この方法は利用される署名機能として National Institute of Standard in Technology Signature Standard (NIST DSS) に限定されていることでも、一般的な用途の点でこの方法

は制限されている。

したがって本発明の課題は、これまで述べてきた欠点を回避するようにした暗号鍵のコンピュータ支援交換方法を提供することにある。

この課題は、請求項 1 に記載の方法により解決される。

本発明による方法により達せられる利点は殊に、公知の方法に比べて本発明に

よる方法の安全性が著しく高い点と、伝送されるメッセージの長さが著しく低減される点にある。本発明による方法によれば、以下のセキュリティメカニズムが実現される：

－ユーザ側とネットワーク側の双方で行われる明示的な認証、すなわち主張する身元識別情報の双方での検証

－双方で行われる暗黙的な認証を伴うユーザ側とネットワーク側との間の鍵の取り決め、すなわち本発明による方法によれば、手順完了後、1つの共通のセッション秘密鍵が利用可能となり、そのうち各々の当事者が知っているのは、認証された相手だけがやはりセッション秘密鍵を所有できるということである。

－ユーザおよびネットワークに対するセッション鍵更新（アップデート）の保証
－ユーザ側とネットワーク側の双方で行われるセッション鍵の承認、すなわち取り決められたセッション

秘密鍵を相手が本当に所有していることの承認

－ユーザの匿名性、すなわち第三者に対するユーザ身元情報の機密性
－ユーザによりユーザからネットワークへ送信されたデータの明白性
－ネットワークからユーザへのネットワーク公開鍵に対する認証の送信
－認証権限からネットワークへのユーザ公開鍵に対する承認の送信

さらに本発明による方法により得られる格別な利点として挙げられるのは、対称暗号化アルゴリズムと比べ著しく計算量の多いモジュラべき乗（modular exponentiation）を各側で2回だけ実行すればよいことであり、このことにより著しく高いプロトコル処理レートが可能となる。

請求項3による本発明による方法の実施形態によれば付加的にさらに別のセキュリティメカニズムが実現され、ユーザ側とネットワーク側との間の公開鍵に対する認証の交換が実現される。

しかも本発明による方法によれば、きわめて容易に種々の要求に整合させることができる。それというのも本発明は特定の暗号化アルゴリズムに限定されるものではないからである。

従属請求項には、以下で詳述する本発明の有利な実施例が示されている。

図1 a, bは、請求項1記載の本発明による方法を表したフローチャートである。

図2 a, bは、請求項3記載の本発明による方法を表した図である。

次に、図1 a, bおよび図2 a, bを参照しながら本発明について説明する。

図1 a, bには、請求項1記載の本発明による方法のシーケンスが描かれている。この方法において前提とするのは、ユーザコンピュータユニットUにおいて信頼できるネットワーク公開鍵 g^s を利用できることである。しかもこの場合、ネットワークコンピュータユニットNにおいて信頼できるユーザ公開鍵 g^u を利用できるものとする。

図1 a, bに示されている本発明による方法は、ネットワークコンピュータユニットNにおける第1の乱数 t の生成から始まる。そしてこの第1の乱数 t から、ネットワークコンピュータユニットNにおいて有限群の生成要素 g により第1の値 g^t が形成される。

非対称の方法は実質的に複雑性理論における2つの問題に基づくものであり、合成数を効率的に因数分解する問題と離散的対数問題(DLP)である。DLPというのは、適切な計算構造においてたしかに指数計算は効率的に実行できるが、逆の演算操作つまり対数計算のためには効率的なアルゴリズムは知られていない、ということである。この種の計算構造は、上述の

有限群のもとで解されなければならない。これはたとえば有限体の乗法的群（たとえばモジュロ p の乗算ただし p は大きい素数）あるいはいわゆる”楕円曲線”である。楕円曲線が注目されるのは殊に、これにより同じセキュリティレベルでも著しく短いセキュリティパラメータが可能となるからである。そしてこれは公開鍵の長さ、証明情報の長さ、セッションキーの取り決めにあたり交換すべきメッセージの長さ、ならびにデジタル署名の長さが該当し、これらについてはあとで説明する。その理由は、楕円曲線に関して既知である対数計算手法は有限体に対するものよりもかなり効率が悪いからである。この関連で大きい素数が意味するのは、是認できる時間内では実行できないほど対数計算が複雑となるよう、素数の大きさを選定する必要のあることである。ここにおいて、”是認できる”

とは、情報技術システムのためのセキュリティ方針に応じて数年～数10年さらにはそれ以上の期間を意味する。

第1の値 g^t の算出後、少なくともこの第1の値 g^t を有する第1のメッセージ $M1$ が形成される。第1のメッセージ $M1$ はネットワークコンピュータユニット N により符号化され、ユーザコンピュータユニット U へ伝送される。そしてユーザコンピュータユニット U において、この第1のメッセージ M が復号される。

さらにユーザコンピュータユニット U において、第

2の乱数 r が形成される。この第2の乱数 r から、選択された上述の計算構造に応じて生成要素 g により第2の値 g^r が算出される。

ユーザコンピュータユニットにおいて利用可能なネットワーク公開鍵は第2の乱数 r により累乗され、これにより第1の中間鍵 $K1$ が生成される。

第1の中間鍵 $K1$ を用いることで、暗号化アルゴリズム E_{nc} を使用してユーザコンピュータユニット U の身元識別情報 $IMU1$ が暗号化される。暗号化された身元識別情報 $IMU1$ により暗号化された第1の項 $VT1$ が形成される。

さらにユーザコンピュータユニット U において、第1の値 g^t をユーザ秘密鍵 u で累乗することにより第2の中間鍵 $K2$ が算出される。

第1の中間鍵 $K1$ と第2の中間鍵 $K2$ に対しビットごとに排他OR関数を適用することにより、セッション鍵 K が算出される。関数 f を利用したセッション鍵 K を用いて、ユーザコンピュータユニット U にもネットワークコンピュータユニット N にも既知であるユーザ定数 $const u$ の暗号化により、第1のレスポンス A が形成される。

この関数 f はたとえば対称暗号関数とすることもできるし、あるいはハッシュ関数または一方向性関数とすることもできる。この関連で一方向性関数とは、所定の関数値に対し合致する入力値を計算することが不

可能な関数のことである。また、ハッシュ関数とは圧縮形の一方向性関数のことであり、ハッシュ関数においては任意の長さの入力キャラクタ列が固定長の出力キャラクタ列にマッピングされる。さらにこの関連で、一方向性関数ないしハッ

シュ関数について不調和がないようにしなければならず、つまり同じ出力キャラクター列を生じさせる異なる2つの入力キャラクター列があつてはならない。既知のハッシュ関数はたとえばMD2アルゴリズムまたはMD5アルゴリズムである。

次に、ユーザコンピュータユニットUにおいて第2のメッセージM2が生成され、その際、メッセージM2には少なくとも第2の値 g^r と、暗号化された第1の項VT1と、第1のレスポンスAが含まれている。第2のメッセージM2はユーザコンピュータユニットUにおいて符号化され、ネットワークコンピュータユニットNへ伝送される。

第2のメッセージM2において伝送される第2の値 g^r によりネットワークコンピュータユニットNは、第1の中間鍵K1を伝送する必要なく第1の中間鍵K1自体を生成することが可能となる。このことが達成される理由は、ユーザコンピュータユニットUとネットワークコンピュータユニットNだけが第1の中間鍵K1を所有しているからである。

第1のレスポンスAはセッション鍵の検証に用いられ、これは後で述べるように、セッション鍵Kを伝送

する必要なくネットワークコンピュータユニットNによつても生成可能である。

ネットワークコンピュータユニットNにおいて第2のメッセージM2の受信後、この第2のメッセージM2が復号される。続いてネットワークコンピュータユニットNにおいて第1の中間鍵K1が計算され、これは第2の値 g^r をネットワーク秘密鍵sで累乗することにより行われる。これによりネットワークコンピュータユニットNは、伝送された第1の暗号化された項VT1を事前に計算された第1の中間鍵K1により解読することができる。

第1の暗号化された項VT1の解読が実行され、これによりユーザコンピュータユニットUは第1のメッセージM2の送信者として認証される。信頼性をもつてネットワークコンピュータユニットNにおいて利用可能なユーザ公開鍵 g^u の累乗から、ネットワークコンピュータユニットNにおいて第1の乱数tを用いることで第2の中間鍵K2が生成される。

セッション鍵KはネットワークコンピュータユニットNにおいてもユーザコン

コンピュータユニットUにおいても、第1の中間鍵K1と第2の中間鍵K2とのビットごとの排他OR結合により算出される。

セッション鍵Kを用い関数fを利用することで第1のレスポンスAが検査される。この検査は、関数fがどのような形式のものであるかに応じて、様々なやり

方で行うことができる。

ユーザコンピュータユニットUにおける明示的な認証は第1のレスポンスAにより達成される。それというのも、ネットワークコンピュータユニットN以外にはユーザコンピュータユニットUだけしかセッション鍵Kを知らないからである。

関数fが対称暗号関数により実現される場合、第1のレスポンスAの検査は2とおりの形式で実施することができる。

ネットワークコンピュータユニットNにとって既知であるユーザ定数constuは、セッション鍵Kを用い関数fを利用することでネットワークコンピュータユニットNにより暗号化することができ、その結果を第1のレスポンスAとそのまま比較することができる。その結果が第1のレスポンスAと一致しているならば、鍵Kの正当性が保証されることになる。

しかし、第1のレスポンスAをネットワークコンピュータユニットNにおいて算出されたセッション鍵を用いて解読することも可能であり、これにより得られた解読されたユーザ定数constu'を既知のユーザ定数constuと比較することができる。ユーザ定数constuが解読されたユーザ定数constu'と一致しているならば、やはりセッション鍵Kの正当性が保証されることになる。

関数fがハッシュ関数により実現されている場合、

第1のレスポンスAの解読は当然ながら不可能である。したがってこの事例の場合には、関数fを利用することでユーザ定数constuとセッション鍵Kにより第1のレスポンスAと比較される結果が送出されるよう、検査を行うことだけが可能である。

次にネットワークコンピュータユニットNにおいて、関数 f を利用することでネットワーク定数 $const_n$ が検査されるセッション鍵 K により暗号化され、第2のレスポンス B が生成される。

さらにネットワークコンピュータユニットNにおいて、少なくとも第2のレスポンス B を含む第3のメッセージ M_3 が生成される。この第3のメッセージ M_3 はネットワークコンピュータユニットNにより符号化され、ユーザコンピュータユニットUへ伝送される。

そしてユーザコンピュータユニットUにおいて第3のメッセージ M_3 が復号され、これに続いて、ネットワークコンピュータユニットNにおける第1のレスポンス A について先に述べたのと同じようにして、第2のレスポンスが検査される。

ユーザコンピュータユニットUにおいてネットワーク公開鍵 g^s が、ネットワークコンピュータユニットNにおいてユーザ公開鍵 g^u が既知でなく、ないしは信頼性を伴って存在していない場合には、請求項3記載の本発明による方法の実施形態が適用される。図2a、bには本発明のこの実施形態が示されている。

ネットワーク公開鍵 g^s とユーザ公開鍵 g^u を交換するために、ユーザ認証子 $Cert_U$ とネットワーク認証子 $Cert_N$ が設けられている場合に有利であるのは、信頼性のある複数の認証権限が存在しているときにユーザコンピュータユニットUがネットワークコンピュータユニットNへ、どの認証権限によりユーザコンピュータユニットUがネットワーク認証子 $Cert_N$ を検証できるのかを通報することである。

このことはたとえば、本発明による方法の開始にあたり認証メッセージをユーザコンピュータユニットUからネットワークコンピュータユニットNへ伝送することにより行える。この関連で認証メッセージは認証コンピュータユニットにおける少なくとも1つの識別情報を有しており、それからネットワークコンピュータユニットNはネットワーク認証子 $Cert_N$ を得ることができ、これをユーザコンピュータユニットUにより検証することができる。

ネットワークコンピュータユニットNが認証コンピュータユニットCAからネ

ットワーク認証子 $Cert_N$ を得た後、そのネットワーク認証子 $Cert_N$ はユーザコンピュータユニット U へ伝送される。

このことは、第1のメッセージ $M1$ に付加的にネットワーク認証子 $Cert_N$ が添付されることにより行われる。この事例の場合、ユーザコンピュータユニット U において第1のメッセージ $M1$ の復号後、ネット

ワーク認証子 $Cert_N$ の検証が行われ、このことでユーザコンピュータユニット U は信頼性のあるネットワーク公開鍵 g_s を得ることになる。

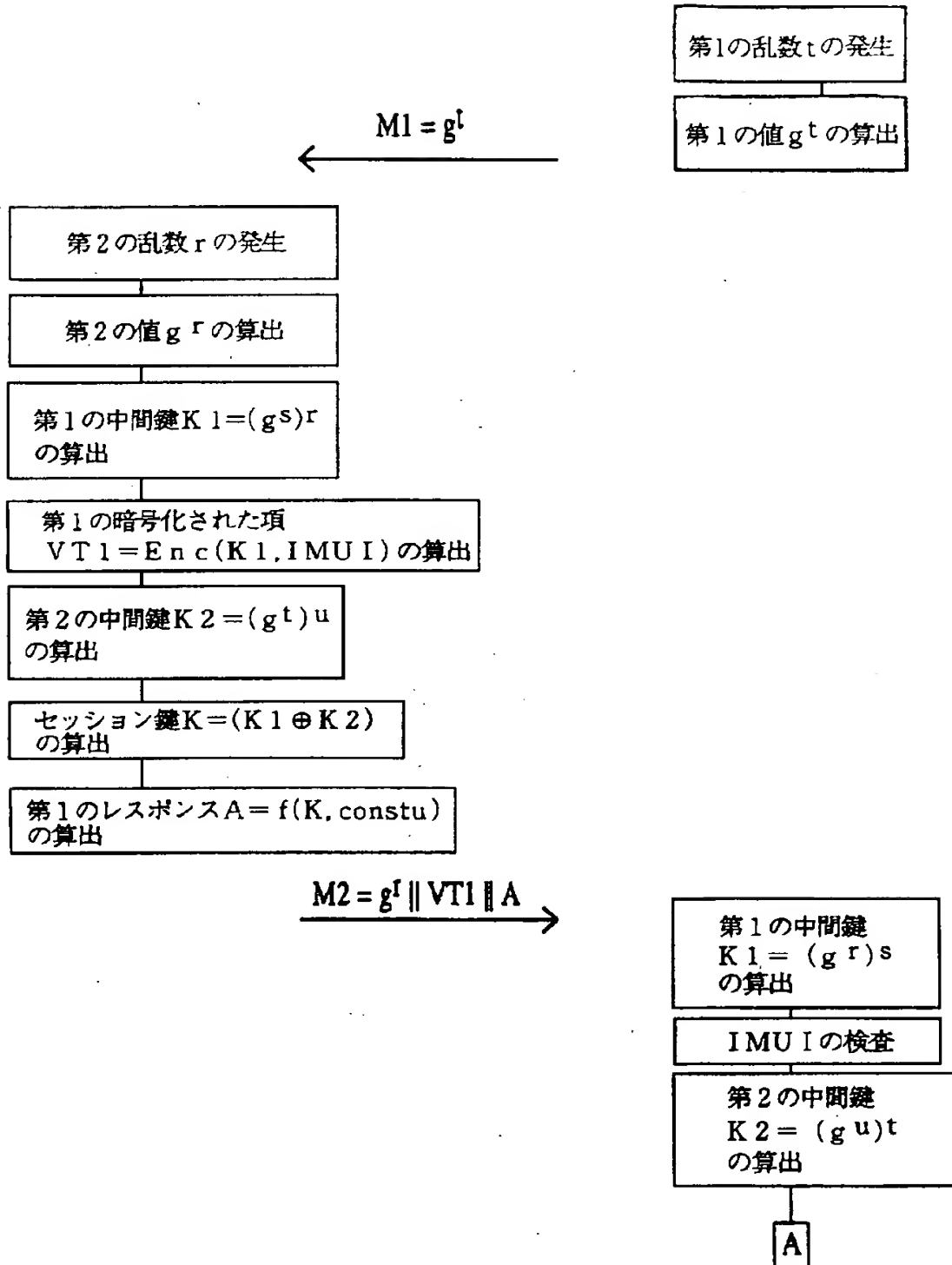
他方、ユーザコンピュータユニット U ではユーザ認証子 $Cert_U$ が求められ、これはユーザコンピュータユニット U の身元識別情報 $IMU1$ の代わりに第1の中間鍵 $K1$ を用い暗号化関数 Enc を利用して暗号化され、第1の暗号化された項 $VT1$ が生成される。このようにして、ユーザコンピュータユニット U の正体が第2のメッセージ $M2$ の伝送時に権限のない第三者のところで明らかにされてしまうことなく、ユーザ認証子 $Cert_U$ の伝送が可能となる。ネットワークコンピュータユニット N において第1の項 $VT1$ が解読された後、このようにして得られたユーザ認証子 $Cert_U$ がネットワークコンピュータユニット N により検証される。このようにして、ネットワーク識別子 $Cert_N$ とユーザ認証子 $Cert_U$ の信頼性のある交換が実現される。

【図1a】

FIG 1a

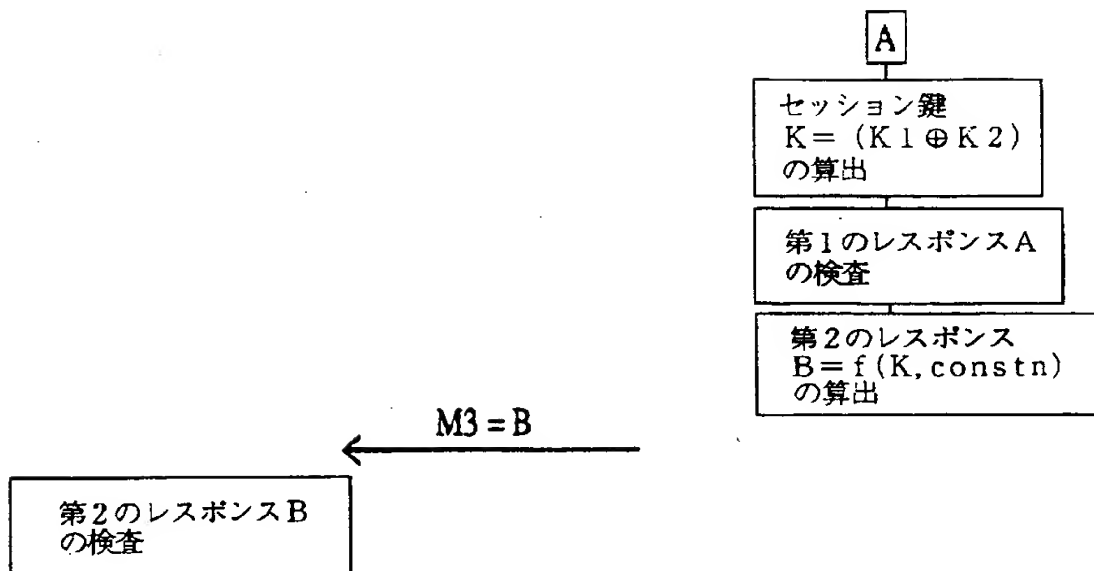
ユーザコンピュータユニットU

ネットワークコンピュータユニットN



【図1】

FIG 1b



【図2】

ユーザコンピュータユニットU

ネットワークコンピュータユニットN

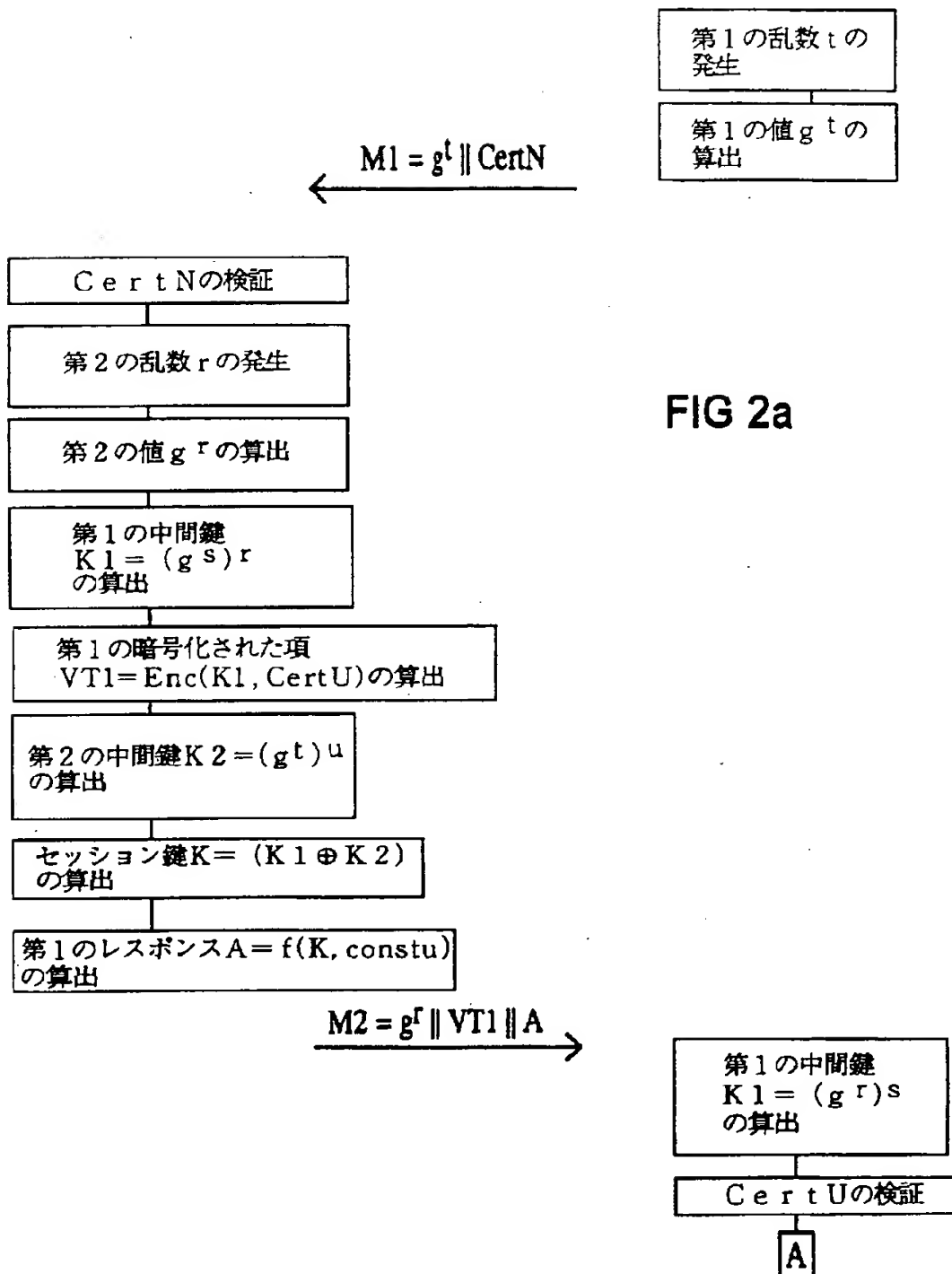
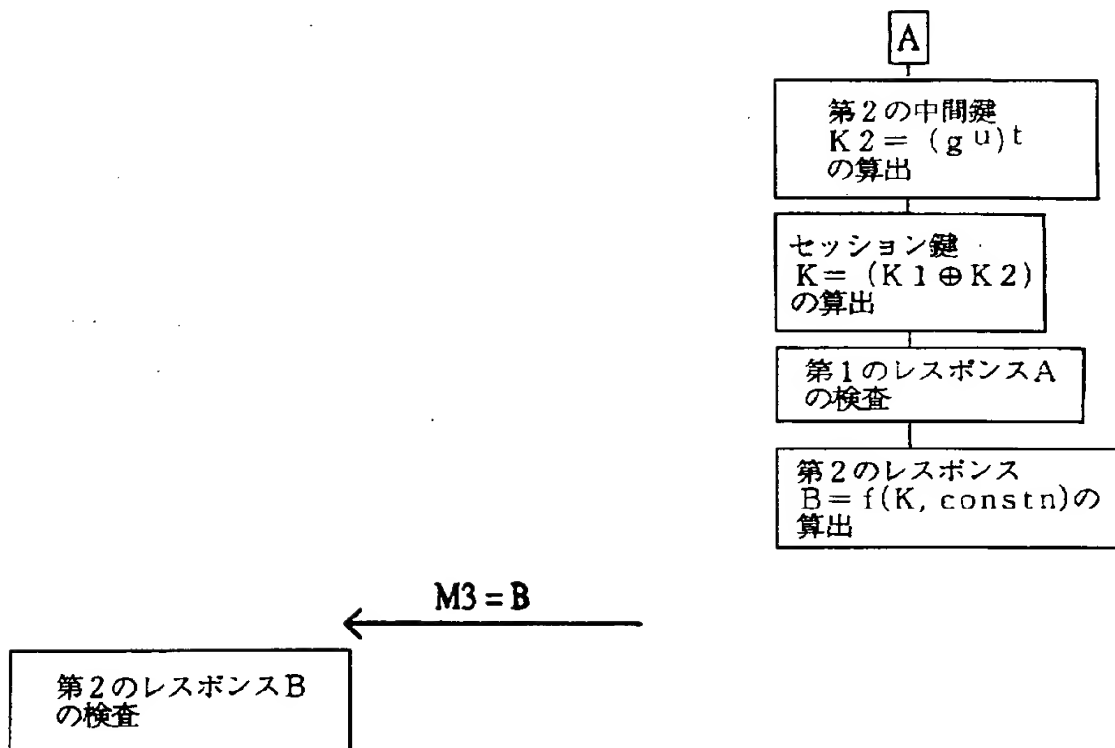


FIG 2a

【図2】

FIG 2b



【手続補正書】特許法第184条の8第1項

【提出日】1997年1月21日

【補正内容】

3. ユーザコンピュータユニット (U) において、前記の第1の中間鍵 (K1) と第2の中間鍵 (K2) とのビットごとの排他OR結合によりセッション鍵 (K) を算出し、

ネットワークコンピュータユニット (N) において、前記の第1の中間鍵 (K1) と第2の中間鍵 (K2) とをビットごとに排他OR結合することによりセッション鍵 (K) を算出する、

請求項1または2記載の方法。

4. ユーザコンピュータユニット (U) において第1のレスポンス (A) を、ユーザ定数 (constu) と前記セッション鍵 (K) に対し関数 (f) を適用することにより生成し、

前記第2のメッセージ (M2) は付加的に少なくとも該第1のレスポンス (A) を有し、

ネットワークコンピュータユニット (N) において該第1のレスポンス (A) を検査する、

請求項1～3のいずれか1項記載の方法。

5. ネットワークコンピュータユニット (N) において第2のレスポンス (B) を、ネットワーク定数 (constn) とセッション鍵 (K) に対し関数 (f) を適用することにより生成し、

少なくとも該第2のレスポンスを含む第3のメッセージ (M3) をネットワークコンピュータユニット (N) からユーザコンピュータユニット (U) へ

伝送し、

ユーザコンピュータユニット (U) において該第2のレスポンス (B) を検査する、

請求項1～4のいずれか1項記載の方法。

6. 方法の開始にあたり認証メッセージをユーザコンピュータユニット (U) か

らネットワークコンピュータユニット (N) へ伝送し、該認証メッセージには認証コンピュータユニットにおける少なくとも1つの識別情報が含まれ、該識別情報からユーザコンピュータユニット (U) により検証可能なネットワーク認証子 (Cert N) を送出させる、

請求項1～5のいずれか1項記載の方法。

7. 前記第1のメッセージ (M1) には、ネットワークコンピュータユニット (N) におけるネットワークコンピュータ鍵 (g^s) のネットワーク認証子 (Cert N) が付加的に含まれ、

ユーザコンピュータユニット (U) において該ネットワーク認証子 (Cert N) を検証し、

ユーザコンピュータユニット (U) において、該ユーザコンピュータユニット (U) におけるユーザ公開鍵 (g^u) のユーザ認証子 (Cert U) を前記第2の中間鍵 (K1) を用い暗号化関数 (Enc) を利用して暗号化することで第1の暗号化された項 (VT1) を生成し、

ネットワークコンピュータユニット (N) におい

て該ユーザ認証子 (Cert U) を検証する、

請求項2または請求項2に依存するかぎり請求項3～6のいずれか1項記載の方法。

8. 前記関数 (f) は対称暗号化アルゴリズム、ハッシュアルゴリズムまたは一方向性関数であり、

ネットワークコンピュータユニット (N) における前記第1のレスポンス (A) の検査にあたり、前記関数 (f) をユーザ定数 (const u) とネットワークコンピュータユニット (N) 内で算出されたセッション鍵 (K) とに対し適用し、その結果を前記第1のレスポンス (A) との整合性について検査し、

ユーザコンピュータユニット (U) における前記第2のレスポンス (B) の検査にあたり、前記関数 (f) をネットワーク定数 (const n) とユーザコンピュータユニット (U) 内で算出されたセッション鍵 (K) とに対し適用し、その結果を前記第2のレスポンス (B) との整合性について検査する、

請求項1～7のいずれか1項記載の方法。

9. 前記関数(f)は対称暗号化アルゴリズムであり、

ネットワークコンピュータユニット(N)における前記第1のレスポンス(A)の検査にあたり、該第1のレスポンス(A)をネットワークコンピュ-

ータユニット(N)において該ネットワークコンピュータユニット(N)内で算出されたセッション鍵(K)を用いて解読し、解読されたユーザ定数(const u')を前記ユーザ定数(const u)と比較し、

ユーザコンピュータユニット(U)における前記第2のレスポンス(B)の検査にあたり、該第2のレスポンス(B)をユーザコンピュータユニット(U)において該ユーザコンピュータユニット(U)内で算出されたセッション鍵(K)を用いて解読し、解読されたネットワーク定数(const n')を前記ネットワーク定数(const n)と比較する、

請求項4または5記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inventor Application No. PCT/DE 96/00591		
A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04L9/08		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Quotation of document, with indication, where appropriate, of the relevant passages	
	Relevant to claim No.	
A	EP,A,0 393 806 (TRW) 24 October 1990 see column 5, line 25 - column 6, line 5 see column 6, line 35 - line 41 see column 10, line 45 - column 11, line 8 ---	1,3
A	IEE PROCEEDINGS-COMPUTERS AND DIGITAL TECHNIQUES, MAY 1994, UK, vol. 141, no. 3, ISSN 1350-2387, pages 193-195, XP000454518 HARN L: "Public-key cryptosystem design based on factoring and discrete logarithms" see page 194, left-hand column, line 27 - line 42 --- -/-	1
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: "A" documents defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" documents referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "d" document number of the same patent family		
Date of the actual completion of the international search 31 July 1996	Date of mailing of the international search report 26.08.96	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 1 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tlx. 31 631 spo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G	

INTERNATIONAL SEARCH REPORT

Internat'l Application No.
PCT/DE 96/00591

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>PROCEEDINGS. THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS 28TH ANNUAL 1994 INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY (CAT. NO.CH3437-1/94), PROCEEDINGS OF IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, ALBUQUER. ISBN 0-7803-1479-4, 1994, NEW YORK, NY, USA, IEEE, USA, pages 76-79, XP000492106</p> <p>WITZKE E L ET AL: "Key management for large scale end-to-end encryption" see page 77, right-hand column, last paragraph - page 78, left-hand column, line 8</p> <p>see page 79, left-hand column, line 37 - line 43</p> <p>-----</p>	1

formation on patent family members

PCT/DE 96/00591

Form PCT-TSA/210 (patent family annex) (July 1992)

フロントページの続き

(72) 発明者 フォルカー ケスラー

ドイツ連邦共和国 D-85256 フィーア

キルヒェン プファラー-シュミッター

シュトラッセ 1